

TINA WOLFSON, SBN 174806
twolfson@ahdootwolfson.com
ROBERT AHDOOT, SBN 172098
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, P.C.
1016 Palm Avenue
West Hollywood, California 90069
Tel: 310-474-9111; Fax: 310-474-8585

LOCKS LAW FIRM, LLC

Michael A. Galpern (*pro hac vice* application to be filed)
Andrew P. Bell (*pro hac vice* application to be filed)
James A. Barry (*pro hac vice* application to be filed)
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200
Fax: (856) 661-8400

Attorneys for Plaintiff and the Putative Classes

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

Dipak Bhuta, individually and on behalf
of all others similarly situated,

Plaintiffs,

v.

Experian Information Solutions, Inc.,

Defendants.

NO. 8:15-cv-1592

**CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

1 Plaintiff DIPAK BHUTA (“Plaintiff”) brings this action against Defendant
2 Experian Information Solutions, Inc. (“Experian” or “Defendant”), on behalf of himself
3 and all others similarly situated to obtain damages, restitution and injunctive relief for
4 the Class, as defined below, from Defendant. Plaintiff makes the following allegations
5 upon information and belief, except as to his own actions, the investigation of his
6 counsel, and the facts that are a matter of public record:
7

8
9 **NATURE OF THE ACTION**

10 1. Plaintiffs bring this class action against Defendant for failing to secure
11 and safeguard the personally identifiable information (“PII”) that Defendant collected
12 and maintained (collectively “Private Information”), and for failing to provide timely
13 and adequate notice to Plaintiffs and other Class members that their information had
14 been stolen and precisely what types of information were stolen (the “Data Breach”).
15

16 2. Due to Defendant’s negligence, the Private Information that Defendant
17 collected and maintained is now in the hands of thieves. Accordingly, Plaintiffs bring
18 this action against Defendant asserting claims for negligence, breach of implied
19 contract, unjust enrichment, and violations of the Fair Credit Reporting Act, 15 U.S.C.
20 1681, *et seq.* (“FCRA”); California Unfair Competition Law, Cal. Bus. & Prof. Code
21 § 17200, *et seq.* (the “UCL”); the New Jersey Consumer Fraud Act (“NJCFRA”),
22 N.J.S.A. 56:8-1, *et seq.*; The New Jersey Data Breach Act, N.J.S.A. 56:8-163, *et seq.*
23 (“NJDBA”); and the California Data Breach Law, Cal. Civ. Code §1798.80, *et seq.*
24 (the “DBL”).
25
26
27
28

PARTIES

3. Plaintiff Dipak Bhuta is a citizen and current resident of New Jersey. Mr. Bhuta signed up for cellular phone service through T-Mobile in or about December of 2014. As part of Mr. Bhuta's agreement to sign up for T-Mobile service, he financed cellular phones, to pay over time. Unbeknownst to Mr. Bhuta, PII related to Plaintiff's application for cellular phone service and financing agreement was passed on to Defendant, Experian. On October 2, 2015 Mr. Bhuta was notified of the fact that Defendant had suffered a theft of the personal identifying information (including names, addresses, birth dates, social security numbers, drivers license numbers and passport numbers) for some fifteen million people who, like Mr. Bhuta, had applied for service with T-Mobile during the past two years.

4. Defendant Experian ("Defendant") is an Ohio corporation with a principal place of business located at 457 Anton Boulevard, Costa Mesa, California 92626. Defendant allowed a massive breach of personal information it collected and maintained to occur, effecting approximately 15 million customers, which is the subject of this Complaint.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises under the FCRA, 15 U.S.C. § 1681 *et seq.*, which is a federal statute.

1 6. This Court also has subject matter jurisdiction over this action pursuant to
2 28 U.S.C. § 1332(d) because the class contains members of diverse citizenship from
3 Defendant and the amount in controversy exceeds \$5 million.

4
5 7. This Court has personal jurisdiction over Defendant because Defendant
6 maintains its headquarters and transacts substantial business in California, and
7 maintains an its principal place of business at 457 Anton Boulevard, Costa Mesa,
8 California 92626, which is in this District.

9
10 8. Venue is proper in this District pursuant to 28 U.S.C. §1391(b)(2) because
11 Defendant maintains offices within this District, and the Data Breach affected
12 consumers in this District.

13
14 **FACTUAL BACKGROUND**

15 **DEFENDANT’S COLLECTION OF PERSONALLY IDENTIFIABLE**
16 **INFORMATION**

17
18 9. Defendant is a consumer reporting agency, which regularly engages in the
19 practice of assembling or evaluating consumer credit information or other information
20 on consumers for the purpose of furnishing consumer reports to third parties on a
21 nationwide basis.

22
23 10. Defendant’s “bureaux hold information about the credit that people and
24 businesses have applied for and their history of repaying it...Each year, [defendant’s
25 bureau]...produce more than 1.2 billion consumer credit reports, that’s close to 3.5
26 million in a typical day...Credit Services contributes 49%* to our global revenue.”
27
28

1 <<https://www.experianplc.com/about-us/our-business-lines/credit-services/>.(last visited
2 October 2, 2015).

3 11. Thus, Defendant stores massive amounts of PII on its servers and utilizes
4 this information to maximize profits.
5

6 **IMPORTANCE OF DATA SECURITY TO PROCESSING OF**
7 **TRANSACTIONS**
8

9 12. Consumers place value in data privacy and trust that their application
10 data, submitted for the purpose of obtaining credit will be kept with the strictest
11 confidence, and under secure conditions. Plaintiffs would not have agreed to apply for
12 credit through a service utilizing Defendant's services or its affiliated entities had they
13 known that Experian does not take all necessary precautions to secure their personal
14 and financial data. Experian failed to disclose its negligent and insufficient data
15 security practices and consumers relied on this omission in providing their personal
16 information in the context of a credit application which would be processed through
17 Defendant's systems.
18
19
20

21 13. Furthermore, when consumers decide to apply for credit or agree to have
22 a credit application processed through a service such as Defendant's, they assume that
23 its data security practices and policies are state of the art and that the provider will use
24 part of the price paid for the service to ensure adequate security measures. In fact,
25 rather than use those moneys to implement data security policies and procedures,
26
27
28

1 Experian simply kept the money to maximize its profits, thus breaching the implied
2 contract.

3 **VALUE OF PII TO COMPANIES AND HACKERS**

4
5 14. Plaintiff's PII is personal property and when stolen, is an extremely
6 valuable commodity. A "cyber black-market" exists in which criminals openly post
7 stolen social security numbers and other personal information on a number of
8 underground Internet websites. This information can be used by thieves to open new
9 financial accounts and take out loans in another person's name, incur charges on
10 existing accounts or clone ATM, debit, or credit cards.
11

12
13 15. PII data has been stolen and sold by the criminal underground on many
14 occasions in the past, and the accounts of thefts and unauthorized access have been
15 the subject of many media reports. Unfortunately, and as will be alleged below,
16 despite all of this publicly available knowledge of the continued compromises of PII
17 in the hands
18 of other third parties, such as retailers, Defendant's approach at maintaining the
19 security of Plaintiffs' and Class Members' PII was lackadaisical, cavalier, reckless,
20 or at the very least, negligent.
21
22

23 **THE DATA BREACH AFFECTING DEFENDANT**

24
25 16. According to T-Mobile:

26 We have been notified by Experian, a vendor that processes our
27 credit applications, that they have experienced a data breach....what
28 we know right now is that the hacker acquired the records of
approximately 15 million people, including new applicants requiring

a credit check for service or device financing from **September 1, 2013 through September 16, 2015**. These records include information such as name, address and birthdate as well as encrypted fields with Social Security number and ID number (such as driver's license or passport number), and additional information used in T-Mobile's own credit assessment. Experian has determined that this encryption may have been compromised.

<<http://www.t-mobile.com/landing/experian-data-breach.html>> (last accessed October 2, 2015)

17. Defendant has not disclosed what other PII it collects or stores were disclosed in the breach, instead providing solely a sample set of categories which may have been disclosed. Without a detailed disclosure, Plaintiffs and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

18. Upon information and belief, Defendant failed to encrypt or maintain its encryption keys on stored PII.

CONSEQUENCES OF DEFENDANT'S CONDUCT

19. Upon information and belief, Plaintiffs' identifying information was disclosed in the Data Breach.

20. The information Defendant lost, including Plaintiffs' identifying information and/or other financial information, is "good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC Interactive Toolkit, *Fighting Back Against Identity Theft*, available at <<http://www.vanderbilt.edu/PersonalIdentityTheftProtection.pdf>> (last visited

1 October 2, 2015). Identity theft occurs when someone uses another's personal
2 identifying information, such as that person's name, address, credit card number, credit
3 card expiration dates, and other information, without permission, to commit fraud or
4 other crimes. *Id.*

5
6 21. As the FTC has stated, once identity thieves have personal information,
7 "they can drain your bank account, run up your credit cards, open new utility accounts,
8 or get medical treatment on your health insurance." FTC, Signs of Identity Theft,
9 available at <<http://www.consumer.ftc.gov/articles/0271-signs-identity-theft>> (last
10 visited October 2, 2015).
11

12
13 22. According to Javelin Strategy and Research, "one in every three people
14 who is notified of being a potential fraud victim becomes one . . . with 46% of
15 consumers who had cards breached becoming fraud victims that same year." Rogers,
16 Kate, Someone Became an Identity Theft Victim Every 2 Seconds Last year available
17 at, [http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-](http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identity-theft-victim-every-2-seconds-last-year/)
18 identity-theft-victim-every-2-seconds-last-year/. (last visited October 2, 2015).
19
20

21 23. Identity thieves can use personal information such as that pertaining to the
22 Class, which Defendant failed to keep secure, to perpetrate a variety of crimes that
23 harm victims. For instance, identity thieves may commit various types of government
24 fraud such as: immigration fraud; obtaining a driver's license or identification card in
25 the victim's name but with another's picture; using the victim's information to obtain
26
27
28

1 government benefits; or filing a fraudulent tax return using the victim's information to
2 obtain a fraudulent refund. This activity may not come to light for years.

3 24. In addition, identity thieves may get medical services using consumers'
4 lost information or commit any number of other frauds, such as obtaining a job,
5 procuring housing, or even giving false information to police during an arrest.

6 25. It is incorrect to assume that reimbursing a consumer for fraud makes
7 that individual whole again. On the contrary, after conducting a study the Department
8 of Justice's Bureau of Justice Statistics ("BJS") found that "[a]mong victims who had
9 personal information used for fraudulent purposes, 29% spent a month or more
10 resolving problems." Victims of Identity Theft, 2012 at 1 (2013), available at
11 <<http://www.bjs.gov/content/pub/pdf/vit12.pdf>> (last visited October 2, 2015). In fact,
12 the BJS reported, "[r]esolving the problems caused by identity theft [could] take more
13 than a year for some victims." *Id.* at 11.

14 26. According to the U.S. Government Accountability Office ("GAO"),
15 which conducted a study regarding data breaches:
16

17 [S]tolen data may be held for up to a year or more before being used
18 to commit identity theft. Further, once stolen data have been sold or
19 posted on the Web, fraudulent use of that information may continue
20 for years. As a result, studies that attempt to measure the harm
21 resulting from data breaches cannot necessarily rule out all future
22 harm.

23 GAO, *Report to Congressional Requesters*, at p. 29 (June 2007), available at
24 <<http://www.gao.gov/new.items/d07737.pdf>> (last visited September 25, 2015).
25
26
27
28

27. While Defendant has not given an indication of the size of the breach at issue, the breadth of its market share indicates that it is substantial, with numerous individuals now facing years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them, and the resulting loss of use of their credit and access to funds whether or not such charges are ultimately reimbursed by the credit card companies.

28. As a result of the disclosure of his Personal Identifying Information, Plaintiff has enrolled in identity theft protection services, at a monthly cost of \$9.99 per month.

CLASS ACTION ALLEGATIONS

29. Plaintiff seeks relief in his individual capacity and seeks to represent a class consisting of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of a class initially defined as follows:

All natural persons and entities in the United States whose personal identifying information was disclosed in the data incursion affecting Experian, which disclosed records related to T-Mobile applications requiring a credit check or device financing between September 1, 2013 and September 16, 2015. (The “Nationwide Class”)

30. Plaintiff also brings this action on behalf of a New Jersey State Class, preliminarily defined as:

All natural persons and entities in the State of New Jersey whose personal identifying information was disclosed in the data incursion

1 affecting Experian, which disclosed records related to T-Mobile
2 applications requiring a credit check or device financing between
3 September 1, 2013 and September 16, 2015. (The “New Jersey
4 Class”)

5 31. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so
6 numerous that the joinder of all members is impractical. While the exact number of
7 Class members is unknown to Plaintiffs at this time, based on information and belief, it
8 is in the millions.

9 32. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of
10 law and fact common to the Class, which predominate over any questions affecting
11 only individual Class members. These common questions of law and fact include,
12 without limitation:
13

- 14 a. Whether Defendant unlawfully used, maintained, lost or disclosed
15 Class members’ personal and/or financial information;
16
- 17 b. Whether Defendant unreasonably delayed in notifying affected
18 customers of the Data Breach and whether the belated notice was
19 adequate;
20
- 21 c. Whether Defendant failed to implement and maintain reasonable
22 security procedures and practices appropriate to the nature and scope
23 of the information compromised in the Data Breach;
24
- 25 d. Whether Defendant’s conduct was negligent;
26
- 27 e. Whether Defendant’s conduct violated the NJCFA;
28
- f. Whether Defendant’s conduct violated NJDBA;

- g. Whether Defendant entered into an implied contract with Plaintiffs and Class Members containing a term to safeguard their Private Information;
- h. Whether Defendant violated the requirements of the DBL;
- i. Whether Defendant's conduct violated the UCL;
- j. Whether Defendant's conduct violated the FCRA;
- k. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

33. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by Defendant.

34. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

35. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

36. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's

1 violations of law inflicting substantial damages in the aggregate would go un-remedied
2 without certification of the Class.

3 37. Defendant has acted or refused to act on grounds that apply generally to
4 the class, as alleged above, and certification is proper under Rule 23(b)(2).
5

6 **FIRST COUNT**

7 **Negligence**
8 **(On Behalf of Plaintiff and All Classes)**

9 38. Plaintiff incorporates the substantive allegations contained in all previous
10 paragraphs as if fully set forth herein.
11

12 39. Plaintiff brings this claim individually and on behalf of the Nationwide
13 Class and the New Jersey Class.
14

15 40. Defendant knowingly collected, came into possession of and maintained
16 Plaintiff's Private Information, and had a duty to exercise reasonable care in
17 safeguarding, securing and protecting such information from being compromised, lost,
18 stolen, misused, and/or disclosed to unauthorized parties.
19

20 41. Defendant had and continues to have a duty to timely disclose that
21 Plaintiff's Private Information within its possession might have been compromised
22 and precisely the types of information that were compromised.
23

24 42. Defendant had a duty to have procedures in place to detect and prevent
25 the loss or unauthorized dissemination of Plaintiff's Private Information.
26

27 43. Defendant systematically failed to provide adequate security for data
28 in its possession.

1 44. Defendant, through its actions and/or omissions, unlawfully breached
2 its duty to Plaintiff by failing to exercise reasonable care in protecting and
3 safeguarding Plaintiff's Private Information within Defendant's possession.

4 45. Defendant, through its actions and/or omissions, unlawfully breached
5 its duty to Plaintiff by failing to have appropriate procedures in place to detect and
6 prevent dissemination of Plaintiff's Private Information.

7 46. Defendant, through its actions and/or omissions, unlawfully breached
8 its duty to timely disclose to Plaintiff and Class Members the fact that their Private
9 Information within its possession might have been compromised and precisely the
10 type of information compromised.

11 47. Defendant's breach of duties owed to Plaintiff and the Class
12 proximately caused Plaintiff's and Class Members' Private Information to be
13 compromised.

14 48. As a result of Defendant's ongoing failure to notify consumers
15 regarding what type of PII has been compromised, consumers are unable to take the
16 necessary precautions to mitigate their damages by preventing future fraud.

17 49. Defendant's breaches of duty caused Plaintiff to overpay for services,
18 purchase services they would not otherwise have purchased, loss of time to monitor
19 and cancel additional cards or accounts, loss of time and money monitoring their
20 finances for additional fraud, diminished value of the services they received, and
21 loss of control over their BAI and/or PII.

1 50. Additionally, Plaintiff is in danger of imminent harm that his PII, which
2 is or may be still in the possession of third parties, will be used for fraudulent
3 purposes.
4

5 51. Plaintiffs seek the award of actual damages on behalf of the Class.

6 52. In failing to secure Plaintiffs' and Class members' Private Information
7 and promptly notifying them of the Data Breach, Defendant was guilty of
8 oppression, fraud, or malice, in that Defendant acted or failed to act with a willful
9 and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiff
10 therefore, in addition to seeking actual damages, seeks punitive damages on behalf
11 of themselves and the Class.
12
13

14 53. Plaintiff seeks injunctive relief on behalf of the Class in the form of an
15 order (1) compelling Defendant to institute appropriate data collection and
16 safeguarding methods and policies with regard to consumer information and (2)
17 compelling Defendant to provide detailed and specific disclosure of what types of PII
18 have been compromised as a result of the data breach.
19
20

21 **SECOND COUNT**

22 **Breach Of Implied Contract** 23 **(On Behalf of Plaintiff and All Classes)**

24 54. Plaintiff incorporates all previous factual allegations as if fully set forth
25 herein.
26

27 55. Defendant, in processing credit check requests, required personal
28 identifying information including but not limited to name, address, date of birth, social

1 security number and a form of secondary identification such as a driver's license
2 number and/or passport number.

3 56. In providing such information, in connection with their credit check
4 requests, Plaintiff and other Class members entered into an implied contract with
5 Defendant whereby Defendant became obligated to reasonably safeguard their
6 sensitive and non-public information.
7

8 57. Defendant breached the implied contract with Plaintiff and Class
9 Members by failing to take reasonable measures to safeguard their PII. Plaintiff and
10 Class Members suffered and will continue to suffer damages including, but not limited
11 to, actual identity theft, fraud and/or phishing, loss of money and costs incurred as a
12 result of increased risk of identity theft, and loss of their PII, all of which have
13 ascertainable value to be proved at trial.
14
15
16

17 **THIRD COUNT**

18 **Unjust Enrichment** 19 **(On Behalf of Plaintiff and All Classes)**

20 58. Plaintiff incorporates all previous factual allegations as if fully set forth
21 herein.
22

23 59. Plaintiff hereby pleads in the alternative to the Second Count.

24 60. Plaintiff and Class Members conferred a monetary benefit on Defendant.

25 61. Defendant received and retained money belonging to Plaintiff and the
26 Class.
27

28 62. Defendant appreciates or has knowledge of such benefit.

63. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members, which Defendant has unjustly received as a result of its unlawful actions.

64. As a result of Defendant's conduct, Plaintiff and the Class suffered and will continue to suffer actual damages including but not limited to, the release of their Private Information; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; and, time spent initiating fraud alerts. Plaintiff and Class members suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, other economic and non-economic losses.

FOURTH COUNT

Intentional Violations of the Fair Credit Reporting Act (On Behalf of Plaintiff and all Classes)

65. Plaintiff incorporates all previous factual allegations as if fully set forth herein.

66. The FCRA requires the proper disposal or transfer of Consumer Information. 15 USCA § 1681w; 16 C.F.R. §682, *et. seq.*

67. In compliance with the FCRA, the FTC codified 16 CFR § 682, *et. seq.*, which regulates the responsibility of companies and individuals who possess Consumer Information. The purpose of the section was to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information. *See* 16 C.F.R. 682.2(a).

1 68. “Consumer Information” is defined as “any record about an individual,
2 whether in paper, electronic, or other form, that is a consumer report or is derived from
3 a consumer report. Consumer information also means a compilation of such records.
4 Consumer information does not include information that does not identify individuals,
5 such as aggregate information or blind data.” 16 C.F.R. 682.1(b).
6

7 69. The Personal Identifying Information disclosed in the Data Breach was
8 Consumer Information pursuant to 16 C.F.R. 682.1 and the FCRA.
9

10 70. 16 C.F.R. § 682.3 requires that “[a]ny person who maintains or otherwise
11 possesses consumer information for a business purpose must properly dispose of such
12 information by taking reasonable measures to protect against unauthorized access to or
13 use of the information in connection with its disposal.”
14

15 71. Disposal is defined as “The discarding or abandonment of consumer
16 information or...the sale, donation, or transfer or any medium, including computer
17 equipment, upon which consumer information is stored.” 16 C.F.R. § 682.1(c).
18

19 72. Defendant is a Consumer Reporting Agency under the FCRA.
20

21 73. Defendant was required to take reasonable measures to protect against
22 unauthorized access while transferring, selling, discarding, or abandoning Consumer
23 Information.
24

25 74. In conscious disregard for the rights of Plaintiff and the Class, Defendant
26 deliberately and/or recklessly did not maintain reasonable procedures designed to
27
28

1 protect against unauthorized access while transferring, selling, discarding, or
2 abandoning the Personal Identifying Information at issue.

3 75. As enumerated above, Defendant's deliberate and/or reckless conduct
4 allowed third-parties to steal, or otherwise access, the Personal Identifying Information
5 without Plaintiff and Class Member's consent and for no permissible purpose under
6 the FCRA.
7

8
9 76. Defendant's conduct violated the FCRA, and Plaintiff and Class Members
10 have been damaged by Defendant's deliberate and/or reckless actions.

11 77. As a result of Defendant's conduct, Plaintiff and Class Members are
12 entitled to actual damages sustained and statutory damages of not less than \$100 and
13 not more than \$1,000, as well as the costs and attorney's fees in bringing this action.
14
15 15 U.S.C. § 1681n.
16

17 **FIFTH COUNT**

18 **Negligent Violations of the Fair Credit Reporting Act** 19 **(On Behalf of Plaintiff and all Classes)**

20 78. Plaintiff incorporates all previous factual allegations as if fully set forth
21 herein.
22

23 79. Defendant was negligent in failing to maintain reasonable procedures to
24 protect against unauthorized access while transferring the Personal Identifying
25 Information.
26
27
28

80. As enumerated above, Defendant's conduct allowed third-parties to steal, or otherwise access, the Personal Identifying Information without Plaintiff's or Class Members' consent and for no permissible purpose under the FCRA.

81. Defendant's conduct violated the FCRA, and Plaintiff and Class Members have been damaged by Defendant's negligent actions.

82. As a result of Defendant's conduct, Plaintiff and Class Members are entitled to actual damages to be proven at trial, as well as the costs and attorney's fees in bringing this action. 15 USC § 1681o.

SIXTH COUNT

**Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §17200, *et. seq.*
(On Behalf of Plaintiff and the Nationwide Class)**

83. Plaintiff incorporates all previous factual allegations as if fully set forth herein.

84. Defendant's conduct constitutes unfair, unlawful and fraudulent business practices within the meaning of the UCL.

85. Defendant's conduct violated certain laws as alleged herein. By engaging in the said conduct in the course of doing business, Defendant engaged in unlawful business practices in violation of the UCL.

86. By engaging in the above-described conduct in the course of doing business, Defendant engaged in unfair business practices in violation of the UCL. The

1 harm to each Plaintiff outweighed any utility that Defendant's conduct may have
2 produced.

3 87. Defendant's failure to disclose information concerning the data breach
4 directly and promptly to affected consumers, constitutes a fraudulent, unfair, and
5 unlawful act or practice in violation of the UCL.
6

7 88. Plaintiff suffered injury in fact and lost property and money as a result of
8 Defendant's conduct.
9

10 89. Plaintiff seeks restitution and injunctive relief on behalf of the Nationwide
11 Class.
12

13 **SEVENTH COUNT**

14 **Violation of the New Jersey Consumer Fraud Act** 15 **N.J.S.A. 56:8-1, *et seq.*** 16 **(On behalf of Plaintiff and the New Jersey Class)**

17 90. Plaintiff incorporates all previous factual allegations as if fully set forth
18 herein.

19 91. Plaintiff brings this claim individually and on behalf of all other New
20 Jersey Class Members.
21

22 92. The NJCFA clearly applies to all New Jersey consumers.

23 93. The NJCFA was enacted to protect consumers against sharp and
24 unconscionable commercial practices by persons engaged in the sale of goods or
25 services. *See Marascio v. Campanella*, 689 A.2d 852, 857 (N.J. Ct. App. 1997).
26
27
28

94. The NJCFA is a remedial statute which the New Jersey Supreme Court has repeatedly held must be construed liberally in favor of the consumer to accomplish its deterrent and protective purposes. *See Furst v. Einstein Moomjy, Inc.*, 860 A.2d 435, 441 (N.J. 2004) (“The [NJCFA] is remedial legislation that we construe liberally to accomplish its broad purpose of safeguarding the public.”).

95. “The available legislative history demonstrates that the [NJCFA] was intended to be one of the strongest consumer protection laws in the nation.” *New Mea Const. Corp. v. Harper*, 497 A.2d 534, 543 (N.J. Ct. App. 1985).

96. For this reason, the “history of the [NJCFA] is one of constant expansion of consumer protection.” *Kavky v. Herbalife Int’l of Am.*, 820 A.2d 677, 681-82 (N.J. Ct. App. 2003).

97. The NJCFA was intended to protect consumers “by eliminating sharp practices and dealings in the marketing of merchandise and real estate.” *Lemelledo v. Beneficial Mgmt. Corp.*, 696 A.2d 546, 550 (N.J. 1997).

98. Specifically, N.J.S.A. 56:8-2 prohibits “unlawful practices” which are defined as:

The act, use or employment of any unconscionable commercial practice, deception, fraud, false pretense, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission whether or not any person has in fact been misled, deceived or damaged thereby.

99. The catch-all term “unconscionable commercial practice” was added to the NJCFA by amendment in 1971 to ensure that the Act covered, *inter alia*,

1 “incomplete disclosures.” *Skeer v. EMK Motors, Inc.*, 455 A.2d 508, 512 (N.J. Ct.
2 App. 1982).

3 100. In describing what constitutes an “unconscionable commercial practice,”
4 the New Jersey Supreme Court has noted that it is an amorphous concept designed to
5 establish a broad business ethic. *See Cox v. Sears Roebuck & Co.*, 647 A.2d 454, 462
6 (N.J. 1994).

7
8 101. In order to state a cause of action under the NJCFA, a plaintiff does not
9 need to show reliance by the consumer. *See Varacallo v. Massachusetts Mut. Life Ins.*
10 *Co.*, 752 A.2d 807 (N.J. App. Div. 2000); *Gennari v. Weichert Co. Realtors*, 691 A.2d
11 350 (N.J. 1997) (holding that reliance is not required in suits under the NJCFA because
12 liability results from “misrepresentations whether ‘any person has in fact been misled,
13 deceived or damaged thereby’”).
14

15
16 102. Rather, the NJCFA requires merely a causal nexus between the false
17 statement and the purchase, not actual reliance. *See Lee, supra*, 4 A.3d at 579
18 (“causation under the [NJCFA] is not the equivalent of reliance”).
19

20
21 103. Defendant’s acts or practice of failing to employ reasonable and
22 appropriate security measures to protect Private Information constitute violations of
23 the Federal Trade Commission Act, 15 U.S.C. § 45(a), which the courts consider when
24 evaluating claims under the Consumer Protection Acts, including N.J.S.A. 56:8-1, *et*
25 *seq.*
26

27
28 **EIGHTH COUNT**

**Violation of the New Jersey Data Breach Act
(On Behalf of Plaintiff and the New Jersey Class)**

104. Plaintiff incorporates all previous factual allegations as if fully set forth herein.

105. The NJDBA provides:

Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

N.J.S.A. 56:8-163.

106. N.J.S.A. 56:8-166 provides that:

It shall be an unlawful practice and a violation of P.L. 1960, c. 39 (C. 56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 [C.56:8-161 through 56:8-164] of this amendatory and supplementary act.

107. As alleged above, Defendant discovered the data breach, however, Defendant failed to notify Plaintiff and Class Members, leaving them to discover the breach through news reports and a press release from T-Mobile.

108. Defendant violated N.J.S.A. 56:8-1, *et seq.* by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the NJDBA, N.J.S.A. 56:8-163, *et. seq.* which provides at Section 163:

Any business or public entity that compiles or maintains computerized records that include personal information on behalf of

1 another business or public entity shall notify that business or public
2 entity, who shall notify its New Jersey customers, as provided in
3 subsection a. of this section, of any breach of security of the
4 computerized records immediately following discovery, if the
personal information was, or is reasonably believed to have been,
accessed by an unauthorized person.

5 109. As a result of the Data Breach, and Defendant's failure to disclose said
6 breach, Plaintiff and Class Members have suffered injury in fact including but not
7 limited to Plaintiff's expenditure of money in order to obtain credit monitoring
8 services.
9

10 110. Defendant's conduct violated the NJDBA, N.J.S.A. 56:8-163, which
11 requires disclosure to affected consumers "in the most expedient time possible and
12 without unreasonable delay."
13

14 111. NJDBA provides that:

15
16 It shall be an unlawful practice and a violation of P.L. 1960, c. 39 (C.
17 56:8- 1 et seq.) to willfully, knowingly or recklessly violate sections
18 10 through 13 [C.56:8-161 through 56:8-164] of this amendatory
and supplementary act.

19 112. As a result of Defendant's violation of New Jersey law, Plaintiff and
20 Class Members are entitled to treble damages, attorneys' fees and costs as well as all
21 other damages the Court deems just. N.J.S.A. 56:8-19.
22

23 **NINTH COUNT**

24
25 **Violation of the California Data Breach Law**
26 **Cal. Civ. Code § 1798.80, et seq.**
27 **(On Behalf of Plaintiff and the Nationwide Class)**
28

1 113. Plaintiff incorporates all previous factual allegations as if fully set forth
2 herein.

3 114. The data breach described above constituted a “breach of the security
4 system” of Defendants, within the meaning of Section 1798.82(g) of the California
5 Civil Code.
6

7 115. The information lost in the data breach constituted “personal information”
8 within the meaning of Section 1798.80(e) of the California Civil Code.
9

10 116. Defendants failed to implement and maintain reasonable security
11 procedures and practices appropriate to the nature and scope of the information
12 compromised in the data breach.
13

14 117. Defendants unreasonably delayed informing anyone about the breach of
15 security of Class Members’ confidential and non-public information after Defendants
16 knew the data breach had occurred.
17

18 118. Defendants failed to disclose to Class Members, without unreasonable
19 delay, and in the most expedient time possible, the breach of security of their
20 unencrypted, or not properly and securely encrypted, personal Information when they
21 knew or reasonably believed such information had been compromised.
22

23 119. Upon information and belief, no law enforcement agency instructed
24 Defendants that notification to Class Members would impede investigation.
25
26
27
28

1 120. As a result of Defendants' violation of Cal. Civ. Code § 1798.80 *et seq.*,
2 Plaintiff and other Class Members incurred economic damages, including expenses
3 associated with necessary credit monitoring.
4

5 121. Plaintiff, individually and on behalf of the Class, seeks all remedies
6 available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages
7 suffered by Class Members as alleged above; (b) statutory damages for Defendants'
8 willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c)
9 equitable relief.
10

11 122. Plaintiff, individually and on behalf of the Class, also seeks reasonable
12 attorneys' fees and costs under Cal. Civ. Code § 1798.84(g).
13

14
15 **PRAYER FOR RELIEF**

16 WHEREFORE Plaintiffs pray for judgment as follows:

17 A. For an Order certifying this action as a class action and appointing
18 Plaintiffs and their Counsel to represent the Class;
19

20 B. For equitable relief enjoining Defendant from engaging in the
21 wrongful conduct complained of herein pertaining to the misuse and/or
22 disclosure of Plaintiff's and Class Members' Private Information, and from
23 refusing to issue prompt, complete and accurate disclosures to Plaintiff and
24 Class Members;
25

26 C. For equitable relief compelling Defendant to utilize appropriate
27 methods and policies with respect to consumer data collection, storage and safety
28

1 and to disclose with specificity the type of PII compromised during the Data
2 Breach;

3 D. For equitable relief requiring restitution and disgorgement of the
4 revenues wrongfully retained as a result of Defendant's wrongful conduct;
5

6 E. Ordering Defendant to pay for not less than three years of
7 credit card monitoring services for Plaintiffs and the Class;
8

9 F. Ordering Defendant to disseminate individualized notice of the Data
10 Breach to all Class members and to post notice of the Breach in all affected stores;
11

12 G. For an award of actual damages, compensatory damages, statutory
13 damages, and statutory penalties, in an amount to be determined;

14 H. For an award of punitive damages, as allowable by law;

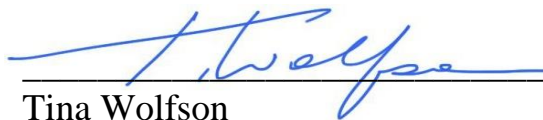
15 I. For an award of attorneys' fees and costs, including expert witness
16 fees;
17

18 J. Pre- and post-judgment interest on any amounts awarded; and

19 K. Such other and further relief as this court may deem just and proper.
20

21 AHDOOT & WOLFSON, PC

22 Dated: October 2, 2015

23 
24

25 Tina Wolfson
26 1016 Palm Avenue
27 West Hollywood, California 90069
28 Tel: (310)474-9111
Fax: (310)474-8585

LOCKS LAW FIRM, LLC

Michael A. Galpern (*pro hac vice* application to be
filed)

Andrew P. Bell (*pro hac vice* application to be filed)

James A. Barry (*pro hac vice* application to be filed)

801 N. Kings Highway

Cherry Hill, NJ 08034

Tel: (856) 663-8200

Fax: (856) 661-8400